Acquisition Scenario – Module 8

TLO 1 **In the context of a DoD IT acquisition scenario, explain the process for obtaining Cloud services**

Module – 8: Summary

Topics

- Module Introduction
- Recapitulation
- Five Step Process
- Acquisition Scenario
- Providers
  - plopBox
  - dockBox
  - milBox
- Discussion
  - plopBox
  - dockBox
  - milBox
- Module Review
- Module Summary Questions

You should be able to:

- In the context of a DoD IT acquisition scenario, explain the process for obtaining Cloud services
- Match foundational cloud terms from the section to appropriate definitions.

Recapitulation of Modules – 1, 2, 3, 4, 5, 6, 7

Topic

Review Previous Content

Content

You should be able to:

Questions

Five-Step Process for Acquiring Cloud Services

Topic

Five-Step Process for Acquiring Cloud Services

You should be able to:

Questions

Content

- Recall that the December 2014 DoD CIO memo summarized (for the mission owner) a five-step process when acquiring cloud services:

1. Perform an IT business case analysis
2. Apply the DoD Cloud Security Requirements Guide
3. Use commercial cloud services that have a DoD Provisional Authorization and a Component Authority To Operate (ATO)
4. Use an approved DoD Cloud Access Point and Computer Network Defense Service Provider to protect sensitive data
5. Apply Defense Federal Acquisition Regulation Supplement (DFARS) Interim Rule to commercial cloud contracts

Perform an IT Business Case Analysis (BCA)

Topic

Perform an IT Business Case Analysis (BCA)

You should be able to:

Questions

Content

- The DoD CIO uses an IT BCA approach to evaluate the acquisition of commercial cloud capabilities
- The DoD Component CIO reviews and approves the individual BCAs
- The DoD Enterprise BCA Template, is intended to facilitate a comparison of alternatives with respect to cost, benefits, operational impacts, and risks
- The BCA can be tailored by the mission owner based on the scope and complexity of the investment
- The December 2014 DoD CIO memo requires that DISA-provided cloud services, such as milCloud, be considered as an alternative in the BCA

Apply the DoD Cloud Security Requirements Guide

Topic

Apply the DoD Cloud Security Requirements Guide,

You should be able to:

Questions

Content

- Recall that the Cloud Computing SRG
  - describes information Impact Levels, which provide a way to categorize the sensitivity of DoD data that can be stored or processed in the cloud
  - specifies the technical architecture requirements for CSOs, guidelines for data recovery and destruction, and Computer Network Defense (CND) requirements
  - specifies physical facility and personnel requirements, including when employees of CSPs must undergo background checks
- The mission owner and mission owner's authorizing official needs to ensure that the security controls for the CSO provides meets or exceeds the security requirements for the information impact detailed by the CC-SRG and the mission's security requirements

CSP/CSO Require PA and Component ATO

Topic

CSP/CSO Require PA and Component ATO

You should be able to:

Questions

Content

- Recall that the PA for a CSO does not automatically allow the mission owner to contract for and/or start storing or processing DoD information in the cloud
- The Component's AO is required to perform the certification and accreditation activities needed to issue the ATO
- The AO should re-use the security package(s) that were submitted in support of DISA's PA review and issuance process
- The mission owner cannot use a CSO to store and/or process DoD until and unless their AO has "signed off" on its use

Use a DoD-CIO approved Cloud Access Point

Topic

Use a DoD-CIO approved Cloud Access Point

You should be able to:

Questions

Content

- Recall that for Information Impact Levels 4 & 5 the CSO must connect to the DODIN through a DoD-CIO approved Cloud Access Point (CAP)
- The CAP provides the necessary cybersecurity and network command and control to protect the DODIN
- The mission owner is required to ensure that a DOD CNDSP provides the required monitoring

Apply DFARS to Commercial Cloud Contracts.

Topic

Apply (DFARS) Interim Rule to commercial cloud contracts.

You should be able to:

Questions

Content

1. Recall that required FAR and DFARS language must be used; in particular the "Network Penetration Reporting and Contracting for Cloud Services" Interim Rule issued 26 AUG 2015
   - Cloud Computing SRG Compliance
   - Contract with the CSP will require CSO provide:
     - Access to Government data for auditing, FOIA, forensic analysis, inspection, and litigation
     - Cyber incident reporting support
     - Damage assessment support
     - Storage of government data in the United States, its territories, or at a location controlled by the United States government
     - CSP personnel that comply with SRG requirements
     - IT service performance in accordance with the Service Level Agreement prepared by the Mission Owner
     - Spillage support
     - Proof that contract terms and conditions flow down to all subcontractors

Acquisition Scenario

Topic

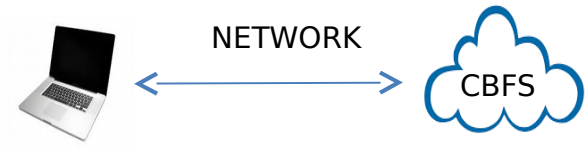
Acquisition Scenario

You should be able to:

Questions

Content

- **Challenge**: As a result of an intensive marketing effort by hypeBox (a commercial cloud storage company) we have been asked to explore what it would take to migrate to a cloud-based file sharing solution (CBFS) and recommend a way-forward for the DoD.
- **Use Case**: From my DoD laptop I want to 'connect' to the CBFS and use it like a local disk drive to archive my emails and store and share my unclassified documents and with other users over the DODIN.
- ***We've been told we must follow current DoD Cloud Policy and use the "5 step process" that it describes.***



Acquisition Scenario – Current Situation

Topic

Acquisition Scenario

You should be able to:

Questions

Content

- Given the volume and variety of documents a determination has already been made that the Information Impact Level is Level 4, **NOT** Level 2
- It has been estimated that there are 3 million users and the average user stores 20 GB of data at cost of $250/year
- Users currently store and share their documents in at least three different ways:
  - 1. Local disk drive; 2. eMail – (e.g. Outlook folders), & 3. Share drives (e.g. network drives, SharePoint, etc.)
- Concerns such as the OPM Breach; insider threats; network intrusions, denial of service attacks, etc. have been voiced as well.
- There are limitations to the current approach
  - Ability to collaborate; excessive document duplication & network traffic, records management, spillage, unreliable backup & restore, etc.

Acquisition Scenario

Topic

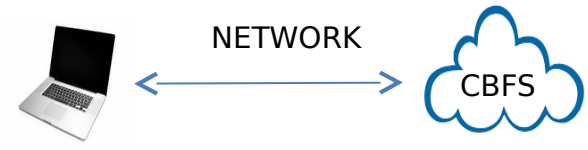
Acquisition Scenario

You should be able to:

Questions

Content

- After an extensive market survey, 3 possible offerings were identified as being able to meet the functional requirements described by the use case
  1. plopBox
  2. dockBox
  3. milBox
- It needs to be determined what the 5 Step Process uncovers in terms of cost, risk, and policy conformance.
- A description of each offerings follows; as you read the description of each try to identify strengths and weaknesses of each alternative. Remember the 5 step process:
  - ✓ Perform BCA
  - ✓ Apply the DoD CC-SRG
  - ✓ DoD PA and ATO to use
  - ✓ Need a CND-SP and connection via a CAP
  - ✓ Must follow DFARS



The three CSOs

Topic

You should be able to:

Questions

Content

- Descriptions follow:

CSO 1: plopBox … offered by a silicon valley start-up

Topic

Vendor: Sili-Start-Up plopBox

You should be able to:

Questions

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, (‘we can see everything’) to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations ‘follow the sun’ and plopBox proudly proclaims, “We hire citizens from the nations in which we do business”
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a ‘no-contract’ monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. “Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)”
6. They have not started the FedRAMP authorization process and they’ve said, “DoD PA?, we can do that and besides, we’ve never been hacked (at least as far as we know)”
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption (‘it’s just few cents per file’)

CSO 2: dockBox … offered by DoD's most buoyant Service

Topic

Vendor: Navy - dockBox

You should be able to:

Questions

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user with no data limit
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

CSO 3: milBox … offered by DISA

Topic

Vendor: DISA - dockBox

You should be able to:

Questions

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP'

Transition to plopBox

Topic

You should be able to:

1. Visual Highlight – used when viewing slides in outline view

Questions

Content

- We will be looking at plopBox closely because it’s an all-commercial CSO and it clearly has problems and risks.

plopBox – Characterize the offering

Topic

Characterization - plopBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. Are the 5 characteristics of cloud met?
   - ✓ **on-demand self-service,**
   - ✓ **broad network access,**
   - ✓ **resource pooling,**
   - ✓ **rapid elasticity,**
   - ✓ **measured service**
   - ➢ **Yes, all characteristics appear to be met**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Characterize the offering

Topic

Characterization - plopBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. What is the NIST Service Model?
   - **This is an example of Software as a Service.**
   - **Although IaaS is a used to support the implementation of the offering, that is opaque to the user.**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Characterize the offering

Topic

Characterization - plopBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. What is the NIST Deployment Model?
   - **This is an example of a Public Cloud**
2. Is it single-tenant or multi-tenant?
   - **multi-tenant**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Characterize the offering

Topic

Characterization - plopBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. What are the architectural elements employed
   1. **The plopBox application**
   2. **The Rain Forest IaaS**
   3. **The Internet**
   4. **The NIPRNET**
   5. **The user's client machine**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 1. Perform BCA

Topic

Discussion – Step 1; Perform BCA

You should be able to:

1. Recognize factors with respect to cost, benefits, operational impacts, and risks needed within the BCA.

Questions

1. What are the costs?
   - **There appears to be a fixed cost of $5/user/month assuming that storage is sold in increments of $5/GB**
   - **There appears to be variable cost of $5/GB/month for each increment**
   - **There appears to be an unknown variable cost for file encryption**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 1. Perform BCA

Topic

Discussion – Step 1; Perform BCA

You should be able to:

1. Recognize factors with respect to cost, benefits, operational impacts, and risks needed within the BCA.

Questions

1. What are some of the benefits?
   - **Low cost per user**
   - **Easy to connect and configure the service**
   - **They have customer support**
   - **They work with the majority of the DoD installed base …**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 1. Perform BCA

Topic

Discussion – Step 1; Perform BCA

You should be able to:

1. Recognize factors with respect to cost, benefits, operational impacts, and risks needed within the BCA.

Questions

1. What are some of the operational impacts?
- -

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 1. Perform BCA

Topic

Discussion – Step 1; Perform BCA

You should be able to:

1. Recognize factors with respect to cost, benefits, operational impacts, and risks needed within the BCA.

Questions

1. What are some of the risks?
   - **Not a mature company, they could easily go out of business if not managed well**
   - **No protection of government data**
   - **Government data hosted in foreign countries that could seize the data or compromise it surreptitiously**
   - **Sharing of IT infrastructure with non-government users, potentially resulting in leakage of information via shared media**
   - **Staff that are not properly vetted**
   - **Acceptance of terms not reviewed by government legal staff could result in the government staff violating federal rules and regulations**
   - **By not completing proper federal government and DoD security assessment and approval process the system will be in violation of government security rules and could result in harm to the government from security compromise**
   - **The organization could overrun its budget**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's ability to comply with DoD assessment criteria
   - **Security vulnerabilities**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's ability to meet required Information Impact Level
- -

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's ability to monitor the system
   - **Unable to mitigate security vulnerabilities**
   - **Unable to comply with DoD requirements for conducting an audit or damage assessment after an attack**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's approach to implementing the system
   - **No protection of government data**
   - **Data centers are not under US government rules or control**
   - **Not staffed with appropriate personnel**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC;
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's approach to connecting the system to the DODIN
   - **Need CAP solution for Level 4 data**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's approach to storing the data
   - -

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC;
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners;
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business;"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card;
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!);"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)."
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's personnel who administer the system
   - **In order to process and store DoD data, CSP must have cleared US persons … not to say they don't but we need to make sure.**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC;
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners;
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business;"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card;
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!);"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)."
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 3. DoD PA and ATO?

Topic

Discussion – Step 3; DoD PA and ATO

You should be able to:

1. Recognized gaps in information, process, or cybersecurity that might limit: DISA's ability to issue a PA; the AO's ability to issue an ATO; and the MO's ability to utilize the CSO.

Questions

1. Identify gaps in information, process, or cybersecurity limiting issuance of a PA:
   - **They seem to be aware of the FedRAMP process, but are not engaged**
   - **They do not appear to understand the requirements for obtaining a DoD PA**
   - **They seem to have a caviler attitude toward protecting their system and users data**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 3. DoD PA and ATO?

Topic

Discussion – Step 3; DoD PA and ATO

You should be able to:

1. Recognized gaps in information, process, or cybersecurity that might limit: DISA's ability to issue a PA; the AO's ability to issue an ATO; and the MO's ability to utilize the CSO.

Questions

1. Identify gaps in information, process, or cybersecurity limiting issuance of an ATO:
   - **No DoD PA, then ATO is really not feasible**
   - **No DoD PA, then no CAP (required for IIL-4)**
   - **Several High Impact security deficiencies**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 3. DoD PA and ATO?

Topic

Discussion – Step 3; DoD PA and ATO

You should be able to:

1. Recognized gaps in information, process, or cybersecurity that might limit: DISA's ability to issue a PA; the AO's ability to issue an ATO; and the MO's ability to utilize the CSO.

Questions

1. Identify gaps in information, process, or cybersecurity limiting use of the CSO:
   - **No CAP, then no data can flow between DODIN and CSO**
   - **No data flow then 'no go' for use**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 4. CAP and CND-SP

Topic

Discussion – Step 4; CAP and CND-SP

You should be able to:

1. Recognized weaknesses in the CSO that might cause harm to the DODIN or limit the ability to monitor activity needed to protect and defend the DODIN.

Questions

1. Identify weaknesses that might cause harm to the DODIN:
   - **Primarily there is no protection at that application layer providing a significant attack vector**
   - **The accreditation of the IaaS provider is unclear**
   - **Insider threat – no cleared personnel in and around the data and infrastructure;**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC;
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners;
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business;"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card;
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!);"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)."
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 4. CAP and CND-SP

Topic

Discussion – Step 4; CAP and CND-SP

You should be able to:

1. Recognized weaknesses in the CSO that might cause harm to the DODIN or limit the ability to monitor activity needed to protect and defend the DODIN.

Questions

1. Identify weaknesses that might limit ability to monitor network and user activity:
   - **No indicated appreciation regarding CS.**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 5. Conform w/DFARS

Topic

Discussion – Step 5; Conform w/DFARS

You should be able to:

1. Recognize business and contracting issues that may factor into the DoD's ability to acquire the CSO.

Questions

1. Identify if the CSO meets the most basic requirements of the Cloud SRG?
   - **It does not appear to meet basic requirements**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 5. Conform w/DFARS

Topic

Discussion – Step 5; Conform w/DFARS

You should be able to:

1. Recognize business and contracting issues that may factor into the DoD's ability to acquire the CSO.

Questions

1. Does the CSO appear to be able to report cyber incidents (IAW the DoD Cloud SRG)?
   - **Requirement to maintain data in the United States unless approved by the AO**
   - **Specify data ownership, licensing, delivery, and disposition instructions**
   - **Unable to identify users**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 5. Conform w/DFARS

Topic

Discussion – Step 5; Conform w/DFARS

You should be able to:

1. Recognize business and contracting issues that may factor into the DoD's ability to acquire the CSO.

Questions

1. Identify where CSO maintains data
   - **US, China, Germany**
2. Does the way data is store meet the requirement of the CC-SRG for IIL-4?
   - **No**
3. Is the MO able to use this CSO without an explicit authorization from the AO
   - **No, the DFARS explicitly requires AO authorization.**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

plopBox – Step 5. Conform w/DFARS

Topic

Discussion – Step 5; Conform w/DFARS

You should be able to:

1. Recognize business and contracting issues that may factor into the DoD's ability to acquire the CSO.

Questions

1. Identify data ownership, licensing, delivery, and disposition instructions
   - **Provides user data to business partners**
   - **If CSP can 'see the data' then they can control the data in ways that cannot be monitored**
   - **Since data is stored in non-US locations it may and probably is subject to non-US law**
   - **SLA's covering other issues need to be put in place; however, given the only option is to accept their terms it's doubtful SLAs could be put in place**
   - **SLA likely violates US procurement rules**

Content

1. plopBox is CBFS as a Service at its finest, they were founded 6 months ago and rated #1 by Gardeners Seed Capital, LLC
2. plopBox contracts with Rain Forest an IaaS provider, ('we can see everything') to host their application and their terms of service allow them to provide user information to their business partners
3. Rain Forest replicates data globally in data centers located in the US, Germany, and China; operations 'follow the sun' and plopBox proudly proclaims, "We hire citizens from the nations in which we do business"
4. They integrate with Windows and Outlook, have tens-of-thousands of anonymous users world-wide, a 'no-contract' monthly pay-as-you-go business model; and they only accept Pay4Play, or major credit card
5. "Set-up is easy … from your browser click 'accept our terms' to install our client software on your PC or mobile device and our servers will do the rest (just make sure your personal firewall is turned off during installation!)"
6. They have not started the FedRAMP authorization process and they've said, "DoD PA?, we can do that and besides, we've never been hacked (at least as far as we know)"
7. They charge $5/user/month for every 5 GB of storage used and offer optional file encryption ('it's just few cents per file')

Transition to dockBox

Topic

Content

You should be able to:

1. Visual Highlight – used when viewing slides in outline view

Questions

dockBox … offered by DoD's most buoyant Service

Topic

Vendor dockBox - Navy

You should be able to:

Questions

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Characterize the offering

Topic

Characterization - dockBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. Are the 5 characteristics of cloud met?
   - o **on-demand self-service,**
   - ✓ **broad network access,**
   - ✓ **resource pooling,**
   - ✓ **rapid elasticity,**
   - ✓ **measured service**
   - ➢ **All characteristics appear to be met by MEGA; however, the need to go through and intermediary (e.g. the Navy and possibly Landing Craft) is not on-demand or self-service.**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Characterize the offering

Topic

Characterization - dockBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. What is the NIST Service Model?
   - **This is an example of Software as a Service.**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Characterize the offering

Topic

Characterization - dockBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. What is the NIST Deployment Model?
   - **This is an example of a Private Cloud**
2. Is it single-tenant or multi-tenant?
   - **single-tenant – the DoD (although there are multiple using organizations)**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Characterize the offering

Topic

Characterization - dockBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. What are the architectural elements employed
   1. **The MEGA SaaS application**
   2. **The Internet**
   3. **The Navy's CAP**
   4. **The NIPRNET**
   5. **The user's PKI enabled Windows machine**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 1. Perform BCA

Topic

Discussion – Step 1; Perform BCA

You should be able to:

1. Recognize factors with respect to cost, benefits, operational impacts, and risks needed within the BCA.

Questions

1. What are the costs?
   - **There appears to be a total per user cost of $200 per year.**
   - **There are no specifics regarding capacity limits or service levels.**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 1. Perform BCA

Topic

Discussion – Step 1; Perform BCA

You should be able to:

1. Recognize factors with respect to cost, benefits, operational impacts, and risks needed within the BCA.

Questions

1. What are some of the benefits?
   - **Low cost per user**
   - **Integrated Windows client**
   - **Navy managed contract and CAP**
   - **They have existing ATOs with the major Services**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 1. Perform BCA

Topic

Discussion – Step 1; Perform BCA

You should be able to:

1. Recognize factors with respect to cost, benefits, operational impacts, and risks needed within the BCA.

Questions

1. What are some of the operational impacts?
   - **It is unclear how an organization could manage its usage and cost for using the dockBox service**
   - **There is no Service Level Agreement with dockBox**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 1. Perform BCA

Topic

Discussion – Step 1; Perform BCA

You should be able to:

1. Recognize factors with respect to cost, benefits, operational impacts, and risks needed within the BCA.

Questions

1. What are some of the risks?
   - **The solution has not yet been assessed and approved by the organization's Authorizing Official**
   - **The government does not have a direct contract relationship with MEGA. They are going through a reseller, Landing Craft**
   - **The description does not describe how the organization can monitor and manage its usage of dockBox**
   - **Unclear how the organization can access its data**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's ability to comply with DoD assessment criteria

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's ability to meet required Information Impact Level
   - **No direct contract relationship with MEGA**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO;
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's ability to monitor the system
   - **The organization has to go through the Navy and Landing Craft to access information about its application on MEGA's system**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's approach to implementing the system
   - **No direct contractual relationship with MEGA**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4.
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed;
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO;
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user.
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'.

dockBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's approach to connecting the system to the DODIN

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's approach to storing the data

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's personnel who administer the system
   - **There appear to be no issues with personnel given the Level 4 DoD PA – those controls were satisfactorily met and verified via the PA process.**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 3. DoD PA and ATO?

Topic

Discussion – Step 3; DoD PA and ATO

You should be able to:

1. Recognized gaps in information, process, or cybersecurity that might limit: DISA's ability to issue a PA; the AO's ability to issue an ATO; and the MO's ability to utilize the CSO.

Questions

1. Identify gaps in information, process, or cybersecurity limiting issuance of a PA:
   - **There appear to be no issues given the Level 4 DoD PA – those controls were satisfactorily met and verified via the PA process. (e.g. FedRamp, DISA PA, Service ATOs) – NCDOC as the CNDSP, etc.**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 3. DoD PA and ATO?

Topic

Discussion – Step 3; DoD PA and ATO

You should be able to:

1. Recognized gaps in information, process, or cybersecurity that might limit: DISA's ability to issue a PA; the AO's ability to issue an ATO; and the MO's ability to utilize the CSO.

Questions

1. Identify gaps in information, process, or cybersecurity limiting issuance of an ATO
   - **The organization's Authorized Official needs to review the existing information/PAs available for the system to determine if additional testing and analysis needs to be conducted for making an assessment of MEGA's CSO security controls**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 3. DoD PA and ATO?

Topic

Discussion – Step 3; DoD PA and ATO

You should be able to:

1. Recognized gaps in information, process, or cybersecurity that might limit: DISA's ability to issue a PA; the AO's ability to issue an ATO; and the MO's ability to utilize the CSO.

Questions

1. Identify gaps in information, process, or cybersecurity limiting use of the CSO:
   - **Need a Component ATO before using the service**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 4. CAP and CND-SP

Topic

Discussion – Step 4; CAP and CND-SP

You should be able to:

1. Recognized weaknesses in the CSO that might cause harm to the DODIN or limit the ability to monitor activity needed to protect and defend the DODIN.

Questions

1. Identify weaknesses that might cause harm to the DODIN:

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 4. CAP and CND-SP

Topic

Discussion – Step 4; CAP and CND-SP

You should be able to:

1. Recognized weaknesses in the CSO that might cause harm to the DODIN or limit the ability to monitor activity needed to protect and defend the DODIN.

Questions

1. Identify weaknesses that might limit ability to monitor network and user activity:
   - **No service monitoring and management facilities have been identified**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 5. Conform w/DFARS

Topic

Discussion – Step 5; Conform w/DFARS

You should be able to:

1. Recognize business and contracting issues that may factor into the DoD's ability to acquire the CSO.

Questions

1. Identify if the CSO meets the most basic requirements of the Cloud SRG?
   - **Yes**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 5. Conform w/DFARS

Topic

Discussion – Step 5; Conform w/DFARS

You should be able to:

1. Recognize business and contracting issues that may factor into the DoD's ability to acquire the CSO.

Questions

1. Does the CSO appear to be able to report cyber incidents (IAW the DoD Cloud SRG)?
   - **Yes**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

dockBox – Step 5. Conform w/DFARS

Topic

Discussion – Step 5; Conform w/DFARS

You should be able to:

1. Recognize business and contracting issues that may factor into the DoD's ability to acquire the CSO.

Questions

1. Identify where CSO maintains data
   - **U.S.**
2. Does the way data is store meet the requirement of the CC-SRG for IIL-4?
   - **Yes**
3. Is the MO able to use this CSO without an explicit authorization from the AO
   - **No, the Interim rule explicitly requires AO authorization; however, given the existing Service ATOs …**

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4.
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO;
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'.

dockBox – Step 5. Conform w/DFARS

Topic

Discussion – Step 5; Conform w/DFARS

You should be able to:

1. Recognize business and contracting issues that may factor into the DoD's ability to acquire the CSO.

Questions

1. Identify data ownership, licensing, delivery, and disposition instructions

Content

- dockBox is Software as a Service owned, operated, and maintained by MEGA (the commercial cloud service provider) for the exclusive use of the DoD certified to Information Impact Level 4
- The Navy and MEGA developed a PKI enabled Windows client as part of the dockBox offering; ATOs for the dockBox offering have been issued by the USN, USA, USAF reusing FedRAMP and DISA assessment and authorization documentation, leveraging reciprocity, and assessing Service specific security controls where needed
- Computer Network defense is provided by NCDOC; MEGA's CSO connects to the DoDIN through the Navy's Cloud Access Point which was approved for use by the DoD CIO
- The Navy acquired MEGA's CSO via one of MEGA's authorized resellers, Landing Craft, a SDVOSBC, for an 'all-in' annual rate of $200 per user
- The Navy handles all transactions with Landing Craft … 'show us the MIPR and you'll be under-way today'

Transition to milBox

Topic

You should be able to:

1. Visual Highlight – used when viewing slides in outline view

Questions

Content

- The 15 Dec 2015 DoD CIO Cloud memo requires that the DISA Services must be considered as an alternative when performing the BCA.
- The discussion that follows is in-line with the preceding plopBox and dockBox discussions.

milBox … offered by DISA

Topic

Vendor milBox - DISA

You should be able to:

Questions

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP'

milBox – Characterize the offering

Topic

Characterization - milBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. Are the 5 characteristics of cloud met?
   - o **on-demand self-service,**
   - ✓ **broad network access,**
   - ✓ **resource pooling,**
   - ✓ **rapid elasticity,**
   - o **measured service**
   - ➢ **No,**

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP'

milBox – Characterize the offering

Topic

Characterization - milBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. What is the NIST Service Model?
   - **This is an example of Platform as a Service**

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP'

milBox – Characterize the offering

Topic

Characterization - milBox

You should be able to:

1. Characterize the CSO according to NIST definitions and recognized the cloud architectural elements employed.

Questions

1. What is the NIST Deployment Model?
   - **Private Cloud**
2. Is it single-tenant or multi-tenant?
   - **-Single Tenant; multiple organizations**

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP'

milBox – Step 1. Perform BCA

Topic

Discussion – Step 1; Perform BCA

You should be able to:

1. Recognize factors with respect to cost, benefits, operational impacts, and risks needed within the BCA.

Questions

1. What are the costs?
   - **$10/Gbytes/month**
2. What are some of the benefits?
   - **IT infrastructure is within direct DOD control and security**
3. What are some of the operational impacts?
   - **Need to establish SOP with DISA since the Component would lose direct control of its IT service**
4. What some of risks?
   - **Infrastructure inadequately provisioned to support the Components requirements**
   - **Level of IT service does not meet Component's needs**
   - **Loss of directly control of Component's mission operations**
   - **Service is more expensive than other options**

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP'

milBox – Step 2. Apply CC-SRG

Topic

Discussion – Step 2; Apply CC-SRG

You should be able to:

1. Recognize where the CSO may fall short in meeting major elements of the CC-SRG.

Questions

1. Identify one or more issues with the CSO's ability to comply with DoD assessment criteria
2. Identify one or more issues with the CSO's ability to meet required Information Impact Level
3. Identify one or more issues with the CSO's ability to monitor the system
4. Identify one or more issues with the CSO's approach to implementing the system
5. Identify one or more issues with the CSO's approach to connecting the system to the DODIN
6. Identify one or more issues with the CSO's approach to storing the data
7. Identify one or more issues with the CSO's personnel who administer the system

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP'

milBox – Step 3. DoD PA and ATO?

Topic

Discussion – Step 3; DoD PA and ATO

You should be able to:

1. Recognized gaps in information, process, or cybersecurity that might limit: DISA's ability to issue a PA; the AO's ability to issue an ATO; and the MO's ability to utilize the CSO.

Questions

1. Identify gaps in information, process, or cybersecurity limiting issuance of a PA:
2. Identify gaps in information, process, or cybersecurity limiting issuance of an ATO:
3. Identify gaps in information, process, or cybersecurity limiting use of the CSO:

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA;
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP.

milBox – Step 4. CAP and CND-SP

Topic

Discussion – Step 4; CAP and CND-SP

You should be able to:

1. Recognized weaknesses in the CSO that might cause harm to the DODIN or limit the ability to monitor activity needed to protect and defend the DODIN.

Questions

1. Identify weaknesses that might cause harm to the DODIN:
2. Identify weaknesses that might limit ability to monitor network and user activity:

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP'

milBox – Step 5. Conform w/DFARS

Topic

Discussion – Step 5; Conform w/DFARS

You should be able to:

1. Recognize business and contracting issues that may factor into the DoD's ability to acquire the CSO.

Questions

1. Identify if the CSO meets the most basic requirements of the Cloud SRG?
2. Does the CSO appear to be able to report cyber incidents (IAW the DoD Cloud SRG)?
3. Identify where CSO maintains data
4. Does the way data is store meet the requirement of the CC-SRG for IIL-4?
5. Is the MO able to use this CSO without an explicit authorization from the AO
6. Identify data ownership, licensing, delivery, and disposition instructions

Content

- milBox is a Platform as a Service, built upon DISA's IaaS, milCloud
- milBox is offered as a DWCF (Defense Working Capital Fund) Service with a $10/GB/month for storage; charges for milCloud infrastructure are included in the rate
- milBox provides all the core services needed to develop and deliver a custom solution tailored to meet specific organizational, user, and capacity requirements. The platform can automatically expand as capacity needs increase
- milBox is certified to Information Impact Levels 5 & 6; The underlying infrastructure and software components are accredited, operated, maintained, and monitored by DISA
- The mission owner AO is required to agree to issuing the ATO for the resulting application
- milBox is connected directly to NIPRNET and/or SIPRNET; 'CAP? we don't need no stinking CAP'

End of box examples

Topic

Content

You should be able to:

Questions

Module - Summary

Topic

Summary

Content

You should be able to:

Questions

Module - Review

Topic

Summary

Content

You should be able to:

Questions

Module 8 - Review

Topic

Summary

Content

You should be able to:

Questions

Module 8 – Summary Questions

Topic

Summary

Content

You should be able to:

Questions